



UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/029,708	12/19/2001	Puqi Tang	10559/594001/P12805	3879

20985 7590 07/22/2005

FISH & RICHARDSON, PC
12390 EL CAMINO REAL
SAN DIEGO, CA 92130-2081

EXAMINER

AST, FATIMA M

ART UNIT	PAPER NUMBER
----------	--------------

2143

DATE MAILED: 07/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/029,708

Applicant(s)

TANG ET AL.

Examiner

Fatima Ast

Art Unit

2143

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 28 April 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,3-12 and 14-30 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,3-12 and 14-30 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Examiner notes that claims 1, 3-6, 8, 12, 14-17, 23-24, 26-27 and 30 have been amended, claims 2 and 13 have been cancelled and no claims have been added.

Claims not explicitly addressed herein are found to be addressed within prior Office Action dated 28 February 2005 as reiterated herein below.

Specification

1. The disclosure is objected to because of the following informalities:
2. The disclosure references drawing element "network 20" on page 4 line 9, however, it appears from the context that the intended reference is to "private network 30". Examiner will assume the intended reference is to "private network 30".
3. Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.
5. Claim 19 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.
6. Claim 19 recites the limitation "wherein determining an access control list" in line 4. There is insufficient antecedent basis for this limitation in the claim. Examiner will assume the intended language is "wherein determining an access control list **entry**".

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claims 1, 3-8, 10-12, 14-19, 21-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rodwin (US 5,812,819) in view of Fan (US 6,219,706) and in view of Srisuresh (US 6,058,431).

9. Regarding amended claims 1, 12 and 23, Rodwin discloses a method comprising, an article comprising a machine-readable medium that stores machine-executable instructions, the instructions causing a machine to and an apparatus comprising: a first memory that stores executable instructions; and a first processor that executes the instructions from the first memory (column 7 lines 31-35) to: determine a private network address for a user in connection with the user accessing a network resource on a network (column 5 lines 20-31).

10. Rodwin does not specifically enumerate determine an access control list entry for the user based on an access control policy and allow or block the user based on the access control list entry, however, Rodwin does disclose a user authentication procedure (column 5 lines 12-20). Fan discloses determine an access control list entry for the user based on an access control policy (column 9 lines 16-31, where an access control policy is identified as a "security access policy"). Fan further discloses allow or block a user based on the access control list entry (column 9 lines 32-40). It would

have been obvious to one of ordinary skill in the art at the time of the applicant's invention to use the access control list of Fan as the authentication procedure of Rodwin in order to gain the advantage of a flexible way to provide access control which is afforded by access control lists (see reference not relied upon "Computer Security Basics" pp 70-72).

11. Rodwin does not specifically enumerate translate a public network address to the private network address for the user accessing the network resource, however, Rodwin does disclose generating a client identifier (column 9 lines 17-38) for the user accessing the network resource, which is forwarded to the server which determines the private network address and further discloses the DHCP server associating each allocated IP address with a handle (column 10 lines 4-13), where the handle is derived from the client id. Srisuresh discloses translating a public network address to a private network address for a user accessing a network resource (column 5 line 51 – column 6 line 11). It would have been obvious to combine the address translation of Srisuresh with the IP address/handle association of Rodwin in to gain the advantage of uniquely identifying and distinguishing the source of a user as disclosed by Srisuresh and Rodwin.

12. Additionally, per applicant's newly amended claim language, Fan does not specifically enumerate sending the determined access control list entry from a first computer on the network to a second computer on the network before allowing or blocking the user access. Fan does teach the device of Fan's invention as a router that may double as a firewall (column 4 lines 45-55) and further teaches the use of access control list entries as noted herein above. Fan also teaches multiple processors and

multiple memories (column 5 lines 31-52). It would have been obvious to substitute a first computer as the firewall of Fan's invention and a second computer as the router of Fan's invention as it is well known in the art to have separate devices in a network to serve as routers and firewalls (see reference not relied upon Teach Yourself Networking in 24 Hours). It would have been further obvious to send the access control list entry from the first computer to the second computer in order to gain the advantage of access control as taught by Fan.

13. Per applicant's newly amended claim language, Rodwin discloses translating the public network address to the private network address after the access control list entry is sent (column 5 lines 10-53, where determining the access control list occurs during authentication, as noted above, and translating occurs during IP address assignment, as noted above).

14. Regarding amended claim 24, per applicant's newly amended claim language, Fan discloses the second processor (column 5 lines 31-52 wherein Fan teaches multiple processors and multiple memories as noted in claims 1, 12 and 23 above).

15. Regarding claims 3, 14 and 25, Fan discloses generating an access control list entry corresponding to the access control policy, that entry including the determined private network address (column 8 lines 11-48, column 1 lines 40-52).

16. Regarding claims 4, 15 and 26, Fan discloses the generated access control list entry comprises a network level access control list including at least one of a destination address, a protocol layer designation, a source port, a destination port, the determined

network address, and an indication of allowed or denied access to the network resource (column 11 lines 45-51, 57-66, column 13 lines 18-25).

17. Regarding claims 5, 16 and 28, Fan discloses the determined access control list entry comprises an application level access control list entry stored on storage device connected to the first computer (column 7 lines 20-40, column 16 lines 64-67).

18. Regarding claims 6, 17 and 27, Rodwin discloses determining the private network address comprises allocating a network address based on a dynamic host configuration protocol (column 5 lines 32-45).

19. Regarding claims 7, 18 and 29, Fan discloses the second computer comprises a network layer device and blocking or allowing access comprises blocking or allowing access at the network layer device (column 4 lines 45-55, column 5 lines 13-22, lines 48-52).

20. Regarding claims 8 and 19, Rodwin discloses a server computer associated with the network resource (column 6 lines 42-45), and an authentication database (column 5 lines 12-15). The combination of Rodwin, Fan and Srisuresh shows an access control list entry further comprises retrieving an application layer access control list entry stored in a database (as noted in claims 5, 16 and 28 above). Rodwin discloses the server computer uses an application layer protocol based on an open system interconnection (OSI) model (column 6 lines 46-66).

21. Regarding claims 10 and 21, Rodwin does not specifically teach releasing the private network address following completion of the access to the network resource, however, Rodwin teaches a DHCP server (column 5 lines 32-44). It is known in the art to

release a private network address which has been assigned by a DHCP server following completion of the access to a network resource (see reference not relied upon, RFC 2131 – Dynamic Host Configuration Protocol).

22. Regarding claims 11 and 22, Fan discloses de-installing an access control entry following completion of the access to the network resource (column 10 lines 19-22, column 15 lines 40-43). Fan does not specifically enumerate that the access control entry which is de-installed is a network layer access control entry, however, as noted in claims 4, 15 and 26 above, Fan teaches the access control entry as a network layer access control entry (column 8 lines 38-59).

23. Regarding claim 30, Rodwin in view of Fan and Srisuresh teaches the network layer device executes instructions to block or allow access to the network resource based on a network level access control list entry as noted in claims 4, 7, 15, 17, 26 and 29 above.

24. Claims 9 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rodwin, Fan and Srisuresh as applied to claims 5 and 16 above, and further in view of Barkley ("Comparing simple role based access control models and access control lists").

25. Regarding claims 9 and 20, Fan discloses storing the access control policy on a storage medium connected to the first computer in the network (column 6 lines 1-10). Fan does not specifically enumerate the access control policy including defined roles for each user allowed to access a resource in the network, however, Fan does teach access control lists (column 9 lines 16-31). Barkley teaches an access control policy

including defined roles for each user allowed to access a resource in a network (I. Introduction p 127). It would have been obvious to combine the defined roles of Barkley with the access control policy of Fan in order to gain the advantages of role based access control as taught by Barkley, including advantage of the opportunity to express an access control policy in terms of the way an organization is viewed.

Response to Arguments

26. Applicant's arguments filed 28 April 2005 have been fully considered but they are not persuasive. Applicant's arguments do not comply with 37 CFR 1.111(c) because they do not clearly point out the patentable novelty which he or she thinks the claims present in view of the state of the art disclosed by the references cited or the objections made. Further, they do not show how the amendments avoid such references or objections.

27. In response to applicant's argument that there is no suggestion to combine Srisuresh with Rodwin and Fan because the nature of the problem to be solved by Srisuresh differs greatly from that of Rodwin and Fan, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, each of the references cited teach some aspect of providing a

user access to a network and the resources therein. Fan teaches an access control system, wherein, among other things, a user's access is determined by an access control list. Rodwin teaches remote access, wherein, among other things, a user's access is determined by IP address and user name. Srisuresh teaches address translation wherein, among other things, a user's access is determined by public and private network addresses. In addition, by applicant's own admission, Rodwin describes an arrangement in which IP addresses may be assigned to a remote network device and Srisuresh teaches an alternative method for such address assignment and translation. It would have been obvious to substitute one means of address assignment for another, as noted in the original office action dated 28 February 2005, and furthermore, it would have been obvious to combine the three references as each of the three references teach the same aspect of network operations, that is access by the user.

28. In response to applicant's argument that there is no suggestion that the router of Fan could act to block or permit access to a network resource, examiner notes that applicant's claims do not contain any indication of a router with the specific functionality of blocking or permitting access and therefore such argument does not address the language of the claims as presented by applicant.

29. In response to applicant's argument that there is no reason for an access control list entry to be sent by a router to a firewall, examiner respectfully disagrees in light of the teachings of Fan. Fan teaches a network device with multiple processors (column 3 lines 64-66), multiple memories (column 6 lines 1-9) and multiple functions (column 4

lines 45-55). Within the network device, an access control list may be sent from one part of the device to another (column 6 lines 1-9 wherein the access control list is stored in one or more memories, column 6 lines 44-63, wherein the firewall code may make use of access control lists stored in "stored information", and further may configure access control lists, column 15 lines 8-42, wherein numerous functional components act upon the ACL and therefore such ACLs must obviously be transferred from one component to another in order for such components to perform the necessary functions, such functions comprising reading, creating, modifying and deleting ACL items). As it is already taught by Fan for ACLs to be transferred among components, if such components are housed in separate devices (as argued by examiner in the rejection of claims 1, 12 and 23 herein above) then it would be obvious for such transfer of ACLs to occur between the devices.

30. In response to applicant's argument that Rodwin, Fan and Srisuresh fail to teach the newly amended features (as noted in the amended claim language) of claims 1, 12 and 23, examiner notes the original rejection has been amended, which amended rejection clearly overcomes applicant's argument.

Conclusion

Examiner has addressed applicant's Amendment, and has further rejected all Amended and Original Claims, as noted herein above. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly,

THIS ACTION IS MADE FINAL. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatima Ast whose telephone number is (571) 272-7217. The examiner can normally be reached on M-F, 8:00-4:30.

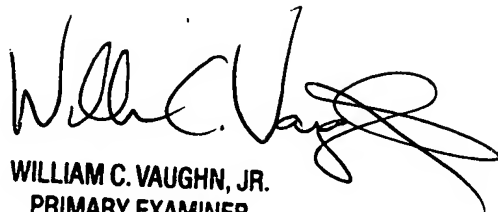
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David Wiley can be reached on (571) 272-3923. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you

Art Unit: 2143

have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Fatima Ast
Examiner
Art Unit 2143

FMA



WILLIAM C. VAUGHN, JR.
PRIMARY EXAMINER